Dificuldades de análise Forense em Mídias SSD

Ademir Silva de Araújo – ademir@phoenixtechnologie.com.br
Computação Forense e Perícia Digital
Instituto de Pós-Graduação - IPOG
Salvador, BA, 29 de Outubro de 2018

Resumo
O presente estudo objetiva analisar quais as dificuldades da análise forense em mídias SSD, a fim de verificar acerca das dificuldades de busca de informação no caso de danos a unidade de armazenamento do tipo SSD. A pesquisa a ser realizada se baseará em um paradigma ontológico, ou seja, partindo da interpretação de uma realidade que será apresentada e estudada no decorrer do trabalho. Assim, a finalidade é explorar uma investigação qualitativa, analisando os conceitos e requisitos que permeiam o contexto da computação forense e da análise de dados e recuperação de informações nos dispositivos que contenham memória flash, sobretudo as mídias SSD. Ademais, serão utilizados métodos sistemáticos e explícitos para recuperar, selecionar e avaliar os resultados de estudos relevantes sobre a dificuldade da observação forense nesse tipo de mídia, de maneira geral e específica, além de reunir e sistematiza os dados dos estudos primários. Já como técnicas de pesquisas, serão utilizadas pesquisas bibliográficas, de modo que se amplie e se conheça as principais contribuições teóricas existentes acerca do tema abordado; pesquisa descritiva não-experimental, de forma a não manipular o fenômeno apresentado pelo tema; além da pesquisa exploratória, a fim de descrever as variáveis que se quer conhecer e explicar, como o estudo dos institutos da computação forense. Por fim, conclui-se que a verificação da dificuldade da análise forense neste campo de atuação, quais sejam, as mídias SSD, é de suma importância para o contexto judicial e extrajudicial e, ainda, para toda a sociedade, não apenas no meio da ciência da computação.

Palavras-chave: Computação. Forense. Memórias Flash. Mídias SSD.

1. Introdução

A tecnologia vem ganhando bastante espaço no cenário mundial, trazendo uma crescente velocidade de informações a partir de inovações ainda mais frequentes. Com isso, uma verdadeira revolução atingiu a memória digital nos últimos anos, através de elementos mais modernos, como, além da unidade de disco rígido já existente, o advento da memória flash, que tem adquirido cada vez mais espaço. Assim, mudanças severas surgiram nos princípios da computação forense a partir do uso da memória flash, em face da grande distinção de como este mecanismo é utilizado na aquisição de PCs a partir do uso de discos rígidos tradicionais. Nesta seara, as informações armazenadas ficam sobremaneira difíceis de serem recuperadas.

Isto posto, houve a popularização da memória flash, tendo em vista a celeridade das suas taxas de dados, o menor custo e a maior resistência a choques, fatores estes que instigam boa parte dos compradores. Contudo, existem malefícios relevantes em tal comparação, como a recuperação de dados, a sua transparência, e, inclusive, no que se refere à análise forense,

diante do efeito crucial que esta apresenta na obtenção de dados forenses e que pode interferir no modo como o a seara judicial utiliza e adquire provas para reter em juízo.

Nesse sentido, a nova tecnologia SSD surgiu para revolucionar a computação forense, trazendo, consigo, aspectos positivos e negativos. Para Scott Moulton (2011), as unidades de estado sólido sobrevieram para destruir os trabalhos forenses e de recuperação de dados. Enquanto os discos rígidos atuais constituem partes não móveis, os chips de memória flash tem o poder de armazenar os dados em vez de discos magnéticos, fator que se mostra como um benefício no consumo de energia, na taxa de dados, e na resistência a choques.

Por um lado, as unidades de disco rígido possuem maior sensibilidade a choques em virtude de suas partes mecânicas, ao passo que os discos de estado sólido têm maior resistência a choques e, logo, são mais próprios para dispositivos portáteis. Em razão da inexistência de partes móveis, se faz necessária uma carga de energia menor para operar os drivers de estado sólido. Este fator, atrelado ao fato de que a duração da bateria destes é maior, com dispositivos mais velozes e resistentes a choques, se refere aos principais motivos pelos quais os atuais computadores portáteis se utilizam de SSDs e não de HDDs.

2. Desenvolvimento

Os *solid-state drivers (SSD)*, ou drives de estado sólido, trouxeram inúmeras alterações significativas na seara da computação forense. É notório o fato de que a utilização, por parte do contexto forense, de uma tecnologia baseada no uso de computadores providos do armazenamento SSD se faz extremamente distinta do modo tal qual aqueles possuidores de mídia magnética tradicional são usufruídos. Nesta senda, tem-se que a segurança e previsibilidade que existia no resgate de informações por aquele suspeito que intentou as apagar foi transformada numa análise incerta, em que não há qualquer certeza de existência de dados ou elementos úteis.

Com isso, as unidades SSD modernas atuam com espaços menores para teorias positivas, visto que a presunção mais cabível é de que poderia um investigador ter acesso aos dados existentes dentro do disco. Assim, nos casos em que o sujeito venha a "destruir" quaisquer arquivos ou informações, através da formatação do disco (inclusive no modo "quick format") ou de forma diversa, estes elementos podem ser perdidos permanentemente em um lapso de tempo muito pequeno. E, ainda que a máquina seja desligada logo após um comando destrutivo ser enviado, há uma possibilidade da destruição das informações no computador, mesmo com a energia restaurada.

É possível afirmar que, com a velocidade do crescimento da memória SSD e tecnologia de controle, bem como com a avançada propagação de fabricantes, unidades e versões de *firmware*, se tornará cada vez mais difícil excluir ou limitar essa inovação dentro do domínio forense e legal. Assim, tudo o que existia no âmbito da recuperação forense e análise de dados apagados e os metadados excluídos podem vir a extinção nesta nova época.

As unidades SSD vem sendo, ao passar do tempo, mais populares, sobretudo em face da alta performance apresentada por estas, com a utilização de componentes eletrônicos e sem qualquer presença de peças movéis. Ao compará-las com o disco rígido, por exemplo, são inúmeros os benefícios apresentados, como, por exemplo, a falta de vibração, de modo a ser executado de maneira absolutamente silenciosa, posto que não há partes móveis; uma resistência maior a choques mecânicos, tendo em vista a inexistência de discos magnéticos

giratórios ou de cabeça de leitura; seu peso que é notoriamente menor; e, por fim, o consumo reduzido de energia, de forma a favorecer sua utilização em dispositivos móveis.

Contudo, cabe pontuar também a inferioridade do disco SSD, em comparação às demais unidades no que tange ao seu custo, posto que se mostra, de forma significativa, mais caro. Essa diferença de valores, no entanto, tem se reduzido nos últimos tempos, de modo que a tendência é que, num futuro próximo, venha a ser possível a substituição com um custo benefício melhor até certa capacidade de armazenamento, visto que, atualmente, a capacidade desses discos alcance 100 TB.

No que diz respeito à organização lógica, os drives de estado sólido atestam a existência de cabeça de leitura e gravação, trilhas e faces de discos, a fim de conservar a compatibilidade com aplicativos que usufruíam do endereçamento de dados através desses elementos característicos.

Ainda numa análise comparativa, tem-se que modelos de memória *flash* possibilita uma quantidade restrita de operações de gravação momentos antes de qualquer desgaste. Por sua vez, as unidades SSD modernas se utilizam de técnicas de nivelamento de degradação inteligente que permitem a gravação em um bloco distinto nos casos em que os dados guardados em um bloco preestabelecido estiverem em processo de alteração, em vez de existir um reaproveitamento de blocos de memória que já existem. Nesta senda, haverão blocos cheios de dados potencialmente delicados esparsados por toda a memória lasca.

Nesse sentido, com o intento de aperfeiçoar o nivelamento de desgaste e expandir a vida útil dos drives de estado sólido, diversos fabricantes tem se utilizado da instalação de *chips* com capacidade de até 25% maior de dados do que os demais discos. Todavia, essa capacidade adicional não é direcionada por intermédio do sistema operacional ou de meio adequado diverso, o que acarreta no fato de que o conteúdo inserido nesse tipo de unidade seja impossível de ser apagado da forma tão segura quanto requerida por determinados padrões governamentais e militares por modos convencionais. Neste seguimento, com o intento de amenizar tal adversidade, certos fabricantes de tal unidade lançaram uma extensão para o ANSI ATA especificação com a finalidade de possibilitar que as informações acondicionadas em todos os chips flash sejam apagadas em segurança.

Para tanto, sobreveio o comando Secure Erase (SE), que, quando implantado de maneira adequada, elimina todo o conteúdo de gerenciamento em um nível de hardware. Via de regra, são os mecanismos seguros de limpeza de software que poderiam substituir os dados inseridos em um disco rígido com informações aleatórias criptograficamente seguras em diversos casos. No entanto, pode ocorrer desses softwares ferramentas serem incapazes de solucionar e de acessar toda a capacidade de armazenamento dos drives de estado sólido. Isto posto, em contrapartida às ferramentas lastreadas em software, o comando ATA Secure Erase irá direcionar controlador embutido no SSD, para apagar eletronicamente os blocos naqueles chips flash .

As unidades SSD que venham a ser apagada, tem seu interior limpo de forma completa, em que todos os blocos ficam totalmente vazios e disponíveis para gravação instantânea, não havendo a necessidade de existirem ciclos adicionais para armazenamento de informações em blocos limpos. Nisto, o comando SE irá restaurar o disco SSD para padrões de fábrica mantendo o seu desempenho de gravação.

Nesse sentido, a fim de exemplificar, tem-se a exclusão feita com total segurança, quando há a implantação adequada, nas unidades SSD de autocriptografia da Intel, em que, conforme a própria empresa, a execução da função SECURE ERASE, como aquelas existentes no Intel® SSD Toolbox, irá fazer com que os drives Intel SSD 320 Series criem uma nova chave de criptografia interna, tornando todos os dados criptografados do usuário inseridos em um Intel 320 SSD da série inutilizáveis de forma quase instantânea, além de fazer isso com os demais dispositivos que suportam criptografia de disco completo no nível de hardware.

Em contrapartida, há a incapacidade de recuperação das informações excluídas de maneira confiável e segura. Isto ocorre porque a utilização do nivelamento de desgaste irá ocasionar em um uso demasiado da capacidade de armazenamento da unidade, se utilizando de blocos de dados livres nas situações em que cada operação de gravação se inicia. A repetição para o mesmo arquivo apenas fará com que todo o conteúdo do drive SSD acabe contaminado, gerando uma queda enfática no desempenho, com velocidades de gravação extremamente reduzidas do que a normal.

A tecnologia flash utilizada nas unidades SSD intenta a exclusão dos blocos antes mesmo que o controlador tenha a possibilidade de executar uma operação de gravação nestes. Apenas os dispositivos baseados na tecnologia flash tem a exclusividade nestas propriedades de armazenamento, sendo bastante distinto da maneira como os tipos tradicionais de mídias magnéticas operam as solicitações de gravação.

Com isso, todo o processo de eliminação dos blocos ocupados anteriormente tem a tendência de ser mais demorado no que tange à leitura e escrita, posto que as unidades SSD que contiverem blocos a serem deletados irão requerer um tempo maior para que seja possível escrever em um único bloco de dados, posto a inexistência blocos vazios. Nesta senda, a coleta de lixo (*garbage collect*) foi pensada pelos fabricantes de SSDs com este fim, qual seja, o de apagar os blocos com dados a serem eliminados e torná-los disponíveis para operações de gravação veloz novamente.

Um dos problemas trazidos pelo mecanismo da coleta de lixo se refere ao fato de que nem as unidades tampouco seus controladores possuem a ciência de quais blocos exatamente são de fato ocupados por arquivos ou estruturas do sistema operacional, e, ainda, quais blocos são inutilizados e estão apenas sujos. Ao passo que o controlador tem a possibilidade de marcar blocos que foram remapeados para blocos diversos como fase de um processo de nivelamento de desgaste, esta informação apenas demoraria o processo da unidade a ser integrada com blocos sujos durante a utilização normal da unidade que, via de regra, abrange a criação, gravação, alteração e exclusão de arquivos.

Na intenção de solucionar tal obstáculo, os projetistas dos drives de estado sólido elaboraram uma interface que possibilita que o sistema operacional, seja este Windows, Linux, Mac OS X, ou outros, possa auxiliar ao controlador acerca de determinados blocos que não possuam mais tempo em uso por meio do comando TRIM. Tal fato propicia a eliminação eletrônica, por meio do coletor de lixo interno, de todos os dados contidos nestes blocos, dispondo-os para operações de gravação futuras. Ainda, cabe ressaltar que os blocos de dados processados pelo coletor de lixo são apagados fisicamente, de modo que tal conteúdo desses blocos não são passíveis de recuperação, ainda que seja utilizado o hardware personalizado. Este fenômeno foi denominado, pelos pesquisadores da área forense, como processo de "auto-corrosão".

Isto posto, a auto-corrosão das unidades SSD fazem com que, atualmente, estes discos se autodestruam, apaguem toda informação a ser recuperada, destruindo, assim, qualquer tipo de evidência judicial. Caso, a máquina, esteja operando garbage collect em segundo plano, isto fará, ao menos na maior parte dos SSDs modernos, com que sejam apagados permanentemente os dados selecionados para exclusão, de maneira que estes se perderão num lapso de tempo absurdamente curto. Ainda que o disco seja redirecionado para outro computador ou anexado a um dispositivo de bloqueio de gravação, a coleta de lixo não terá como ser bloqueada. Com isto, a única forma de evitar a auto-corrosão seria separar fisicamente o controlador de disco do flash chips de memória, conservando seus dados e, após, acessando os chips de forma direta via hardware personalizado.

No que se refere à volumes criptografados e unidades SSD, salienta-se que estes não possuem bom desempenho juntos, posto que haverá um desgaste decorrente exatamente dos problemas de desempenho supracitados. Existem algumas configurações em que os contêineres criptográficos criptografam por completo o espaço presente no disco, inclusive o espaço livre, de modo que cada gravação realizada nesta unidade será uma reescrita, diminuindo de maneira significativa o desempenho de gravação em SSDs.

Acerca do exposto, os desenvolvedores de aplicação de criptografia identificaram tal problematização e adotaram meios de solucionar a questão, como diversos tipos novos de configurações e opções avançadas. Nisto, foi possível a liberação de espaço não utilizado de volta ao controlador SSD, o que gerou um enfraquecimento da segurança geral.

Então, a partir da criação de um volume criptografado com capacidade fixa, o comportamento padrão será no sentido de criptografar todo o conteúdo de um arquivo que representa o volume criptografado Isto fará com que o efeito do Comando TRIM seja desativado para o conteúdo do volume criptografado. Quanto a este assunto, cabe afirmar que em muitas configurações, sobretudo naquelas padrões, os arquivos excluídos referentes a volumes criptografados não serão ameaçados pelo comando TRIM.

Para se ter um computador criptograd tem que manter um par de chave original da decodificação em cache de memoria que pode ser removida através de um Live RAM obtido de um computador executando um ataque Firewire.

As referidas chaves também podem estar presentes em arquivos de paginação ou arquivos de hibernação. Existem, inclusive, outros métodos como o disco forense “Elcomsoft O Decryptor” que tem a possibilidade de extrair arquivos de descriptografia de despejos de memória e arquivos de páginação ou hibernação e de descriptografar o conteúdo de volumes criptografados.

Nesse interím, as unidades SSD podem ser acopladas diretamente à interface SATA do PC ou conectada por intermédio de um dispositivo de bloqueio de gravação similar ao utilizado para verificar discos rígidos magnéticos. Assim, ao passo que os bloqueadores de escrita impossibilitam as alterações nos dados conservados no disco SSD, a sua relação com a operação do comando TRIM e o coletor de lixo interno do disco é ínfima. Entretanto, ressalta-se que a unidade SSD conectada através de um dispositivo de bloqueio de gravação seguirá executando o lixo de fundo coleção, o que, provavelmente, pode vir a eliminar os últimos indícios de dados que já tenham sido apagados da unidade.

Em consequência, cabe aludir acerca da forma de perícia relativa ao disco SSD. Os drives de estado sólido tem o poder de auto-destruir provas judiciais, tornando a extração de arquivos ou dados já apagados quase que impraticável. No entanto, a técnica de aquisição

adequada pode ocasionar na geração das chaves originais de decodificação binária, de modo a possibilitar que investigadores tenham acesso à dados armazenados em volumes criptografados.

Ainda, resta salientar a existência de certas exceções que tem o condão de impedir a presença de elementos com evidência de auto-destruição em unidades SSD. Nos dias de hoje, os drives de estado sólido utilizados em dispositivos NAS, participando de RAID configurações, e conectados como dispositivos externos via USB e FireWire também estão isentos de qualquer evidência de autocorrupção. Também, as versões mais antigas do Windows, Mac OS e Linux são exceções pois não suportam mecanismos de coleta de lixo em unidades SSD.

A sistemática da coleta de lixo irá atuar concomitantemente à funcionalidade TRIM. Isto se dá porque este rastreia as células a serem apagadas e pode interligar demais informações de células distintas em células vazias para eliminar outras. Tal processo se dá quase que de forma total em segundo plano e apenas há a suspeita de cooperação com o TRIM.

A expectativa é que esses drives de estado sólido distintos apresentem um desempenho distinto na exclusão das informações, apagando apenas um subconjunto dos blocos, e não todos de uma só vez.

De outra forma, as unidades de disco rígido convencionais tem capacidade de conservar dados em discos giratórios feitos de alumínio ou vidro, envoltos com um material magnético fino. Esses discos giram em virtude de um motor que é colocado em um eixo por meio de um orifício no centro do disco e, a depender da execução, terá uma velocidade variável entre 6.000 e 10.000 rotações por minuto. Em computadores de mesa, a velocidade de 7.200 rpm é padrão, ao passo que em aplicações que possuam um desempenho alto, 10.000 rpm é apenas habitual. Com isso, os fornecedores se utilizam de quantidades distintas desses discos empilhadas uma sobre a outra com a finalidade de multiplicar o espaço de armazenamento.

Existe, dentre os discos supracitados, o braço do atuador ou o controle deslizante que se move e, neste controle deslizante, é montada uma cabeça de leitura e de gravação. Esse braço do atuador conecta as cabeças através dos *bits* magnetizados, ocasionando uma espécie de voo destes sobre a superfície de fiação, tendo, esta, que ser bastante lisa, para que a leitura das cabeças possa ser realizada de modo uniforme.

Tal efeito apenas é aplicável enquanto os discos estão em movimento, ou, de outro modo, a cabeça irá entrar em contato com o disco. A fim de dificultar o referido contato, são utilizadas duas formas de abordagem. Inicialmente, as unidades anteriores se valiam da zona de pouso, termo denominado para um pequeno anel localizado no disco próximo ao centro com uma textura mais propícia. A cabeça seria, então, deslocada pelo braço para este anel em momento anterior que o inversor desligasse e os discos parassem de circular.

Por outro lado, as unidades mais modernas se utilizam de rampas para descarregar as cabeças, sendo o braço empurrado por uma rampa que levanta as cabeças e as coloca em uma posição de estacionamento. Logo após, os discos passarão a girar com determinada velocidade, de modo que as cabeças irão se mover em direção aos discos. Assim que alcançarem a velocidade necessária, a cabeça irá flutuar acima do disco em virtude de suas propriedades aerodinâmicas.

Dificuldades de análise Forense em Mídias SSD

Julho/2019

De pronto, cabe afirmar que a cabeça de gravação, mais conhecida como cabeça indutiva de filme fino, ou cabeça TFI, constitui-se em uma bobina de filme fino que concede um campo magnético no momento em que a corrente passa pela bobina. O núcleo, que é o elemento no qual a bobina se encontra, possui uma pequena lacuna no fundo. Esta sobrevoa a superfície do disco e tem a possibilidade de alterar a polarização da área no disco que, por sua vez, passa modificando a polarização da corrente pela qual a bobina se encontra.

Seguindo o mesmo princípio, mas, desta vez, executando de forma invertida, a cabeça de leitura funcionará como uma bobina de filme fino enrolada ao redor de um núcleo mais estreito do que o da cabeça de gravação. A bobina se utilizará do efeito magneto-resistivo de modo que este irá captar a polarização do bit anterior e mandar uma corrente, que poderá ser traduzida em zero ou um bit.

Quanto à disposição dos dados nos discos rígidos, salienta-se que a menor unidade de informação gravada em mídia magnética é um bit. O conjunto de bits, por sua vez, é disposto em formas circulares, formando trilhas em torno do disco. Um disco rígido típico possui 70.000 a 100.000 faixas em cada uma de suas superfícies.

Para que uma nova trilha possa ser escrita, a cabeça de gravação é arrastada pelo braço para a próxima posição no raio. Todas informações são escritas em blocos de dados de 512 bytes, ficando estes gravados sequencialmente ao longo da faixa. Uma cabeça distinta é utilizada em outra superfícia, posto que um disco rígido se refere a vários discos graváveis em ambas as superfícies e apenas um braço atuador, existindo vários controles deslizantes e cabeças.

Nesta disposição, todas as cabeças têm posição similar em sua superfície de acordo, de modo que a pista mais externa em qualquer superfície é a pista 0 e, com isso, todas as trilhas 0 juntas são denominadas cilindro 0. A partir da utilização de endereços de cilindro, os fabricantes tem a chance de elevar as velocidades de acesso, posto que diversos cabeçotes podem ler de maneira simultânea. Cada uma dessas faixas é dividida em setores, denominados de servo setores. Tem-se que cada setor possui, geralmente, a capacidade de 512 bytes, endereçados a partir de 1 para cada faixa. Com o intento de verificar setores e trilhas, padrões magnéticos especiais são gravados no disco durante a produção.

O método de endereçamento CHS, Cylinder-Head-Sector, pode ser usado para tratar de um setor específico. A partir deste método, um setor pode ser encontrado pelo cilindro (a partir de 0), a cabeça da superfície de acordo (a partir de 0) e o número do setor (a partir de 1). Todavia, este método de endereçamento foi substituído pelo LBA, isto é, *Logical Block Addressing*.

Deve haver uma formatação do disco e a criação de uma partição antes que os dados possam ser inseridos em um disco por um sistema operacional. Uma partição se trata de uma unidade lógica que separa o disco em partes lógicas distintas. No *Master Boot Record* (MBR), armazena-se uma tabela de partição no primeiro setor do disco, comunicando ao sistema operacional como é a divisão do disco. Alguns sistemas operacionais como Linux, Windows ou Macintosh dispõem de diferentes sistemas de arquivos nas partições. Ao passo que o Windows usa FAT, o NTFS Linux usa EXT2 ou EXT3. Dessa forma, um sistema de arquivos irá seguir o local no disco físico em que os dados são guardados.

É utilizada pelo Windows uma tabela de arquivos mestre, denominada tabela MFT, figurando como uma espécie de índice para os arquivos que são conservados em discos rígidos. Cabe afirmar que o simples fato de se eliminar uma partição ou reformatá-la não

causa qualquer interferência com os dados reais. Somente são excluídos a tabela de alocação de arquivos (denominada FAT), mas os dados ainda tem chance de serem resgatados.

Concernente à memória flash, salienta-se que sua velocidade, eficiência em termos de energia e maior resistência a choques se dá pela ausência de partes móveis, visto que inexiste discos giratórios ou cabeças móveis lendo e gravando em um só disco. Esses dispositivos de memória flash são sistemas pequenos e completos, nos quais cada componente é soldado a uma placa de circuito impresso, chamada de PCB. As memórias semicondutoras, que são memórias flash, podem ser separadas em duas categorias principais, sendo estas, a RAM, que é a memória de acesso aleatório, e a ROM, que é a memória somente leitura. As informações contidas na memória da ROM apenas podem ser gravadas e serão armazenadas virtualmente por toda a vida útil do disco. Por sua vez, a memória RAM é regravável e perde seus dados no exato momento em que o dispositivo não dispor mais de energia.

As memórias não voláteis (NVM) surgiram na década de 1970, em que os dados armazenados por estes dispositivos podem ser alterados, mas também são conservados depois do desligamento. Estas passaram a ter aplicação em memórias flash usadas para cartões USB e cartões de memória flash a partir da década de 1990.

As memórias flash apresentam dois tipos distintos, quais sejam, NAND e NOR. Primeiramente, tem-se que são baseados na memória NAND as memórias flash como cartões SD, drives USB e SSDs. Estas possuem suas células lastreadas na tecnologia Floating Gate (FG), como a memória NOR, não obstante o fato de que os chips NAND possuam tamanho menor e sejam mais velozes, custando uma média de 60% do valor de um chip NOR semelhante a ser produzido. Em contraponto, nem toda célula pode ser escrita e excluída de maneira independente, tendo que ser gerenciada em matrizes de bytes, setores e blocos, enquanto que os chips NOR comandam cada célula independentemente.

Uma célula NAND é produzida com duas portas sobrepostas, em que uma é totalmente cercada por óxido e a outra formará o terminal da porta. Caso a voltagem seja executada na porta de controle, os elétrons podem passar da fonte pelos dielétricos e cair na porta flutuante. Eles permanecerão presos e podem ser conservados por muitos anos. A carga da célula de neutra, então, será alterada para negativa e é denominada de programação. Apenas se a voltagem for aplicada ao dreno, os elétrons irão do portão flutuante e regressarão a célula para o neutro. Cada célula possuía um bit de informação (célula de nível único, SLC) até que as células multicamadas (MLC) fossem inventadas, as quais possuíam dois ou mais bits.

Estas células encontram-se interligadas a matrizes. Um array geralmente consiste em 8192 blocos, onde um bloco contém 64 páginas (4000 + 128 Bytes). Nesta memória NAND, uma operação de gravação pode ser realizada em nível de página, mas, em face de restrições de hardware, os comandos de exclusão sempre afetam blocos inteiros.

Quanto ao controlador de memória SSD, tem-se que, não obstante existam muitos fornecedores vendendo unidades SSD, são poucos os controladores de SSD que de fato o produzem. Em regra, os fornecedores de SSDs passaram a comprar controladores de outras empresas e adequam seus próprios chips ou outros chips de memória NAND com eles.

São poucas as empresas que produzem controladores, de modo que aumenta sobremaneira a concorrência entre os fabricantes. Alguns fatores distinguem um SSD de outros chips de memória, como as rotinas internas do controlador de memória, a implementação do nivelamento de desgaste e coleta de lixo, compactação e criptografia, o que

interfere de maneira direta as velocidades de leitura e gravação dos drives. Por este motivo, a discrição dos fabricantes é muito mais forçada sobre seus próprios.

Os drives de estado sólido apresentam, ainda, uma relevante função que o diferencia dos HDDs, que é o comando TRIM. Este se refere a um atributo do comando de gerenciamento do Conjunto ATA e possibilita que o sistema operacional comunique ao SSD os blocos a serem excluídos. Assim, o TRIM informará ao dispositivo a listagem dos blocos que são seguros para remoção.

O comando supracitado é habilitado por padrão usando o Microsoft Windows 7 ou o Windows Server 2008, porém pode ser desabilitado ou habilitado também por outros comandos no prompt de comando do Windows. Nenhuma outra ação é necessária, posto que a função é ativada por padrão nos sistemas operacionais que suportam TRIM, exceto para desabilitar o TRIM de forma proposital com finalidade de teste.

No entanto, existe um nivelamento de desgaste nestes tipos de dispositivo. Deste modo, tendo em vista que cada célula NAND inserida em um chip flash possui uma vida útil limitada. Há um número restrito de ciclos de gravação, em regra assegurados para suportar mais de cem mil ciclos. No geral, nem todos os dados contidos em um dispositivo sofrem alterações com a mesma frequência, visto que alguns dados são atualizados com certa frequência, ao passo que outros dados podem não ser alterados por um período de tempo maior. Se faz crucial manter o envelhecimento de todas as células uniformes e ao mínimo, a fim de superar a degradação de algumas células e deixar outras intocadas. Para tanto, são duas as abordagens existentes, quais sejam, nivelamento de desgaste dinâmico e estático.

O nivelamento de desgaste dinâmico remapeia os endereços LBA do sistema host para a página posterior livre quando o host salva na unidade ou atualiza os dados em uma página. Essas informações sempre serão armazenadas na próxima célula livre com o menor nível de envelhecimento. Logo, por meio do nivelamento dinâmico, as células que não foram modificadas permanecerão intocadas, de modo que o uso igual não é garantido.

Já o nivelamento estático faz o mesmo processo do nivelamento dinâmico, mas, além disso, também move páginas estáticas periodicamente para outras páginas. Assim, as informações em uma das páginas podem ser movidas para outra página a fim de liberar a célula e torná-la utilizável para novos dados. Nesse sentido, na intenção de diminuiro impacto no desempenho, o nivelamento de desgaste é feito em segundo plano, sobretudo enquanto a memória está no modo de espera.

Com a mapeação de um endereço LBA para uma nova página, ou no caso do sistema de arquivos ter instruído a memória a apagar um endereço, a página não será excluída instantaneamente, mas sim selecionada para ser excluída a partir do uso do comando TRIM. Isso ocorre em face da restrição de hardware NAND, acima abordada, em que um bloco que contenha diversas páginas tenha a capacidade de armazenar mais informações do que aquelas apagadas. Nesta situação, a rotina de coleta de lixo controla as páginas apagadas e exclui blocos inteiros quando este se encontrar pronto para ser excluído.

Caso um desses blocos possua muitos arquivos a serem apagados ou outros blocos vazios precisem ser criados, a coleta de lixo irá mover as páginas faltantes para páginas distintas antes de excluir o bloco. Neste processo, os dados restantes de blocos a serem apagados serão combinados em blocos vazios para que outros possam também ser excluídos. Ressalta-se que tal operação é feita em segundo plano e atua como o nivelamento de desgaste não visível para o sistema host.

Revista On-Line IPOG
ESPECIALIZE

Dificuldades de análise Forense em Mídias SSD

Julho/2019

Embora existam três tipos principais de memórias flash, cada um com sua própria aplicação alvo e, assim, forma de implementação, características e arquitetura ligeiramente distintas, as funções e rotinas supracitadas, via de regra, são iguais para todos os flash memórias. No entanto, todas as memórias flash necessitam conter um nivelamento de desgaste coleta de lixo, mas suas implementações modificam de fornecedor para fornecedor.

O primeiro tipo de memória flash se refere aos cartões Secure Digital, também denominados cartões SD. Estes surgiram no final de 2001 e trouxeram uma memória flash otimizada para um dispositivo em formato pequeno, com processos de escrita veloz de arquivos relativamente pequenos. Todos estes cartões SD foram criados para utilização de arquivos com formato FAT / FAT32 / exFAT / NTFS e possuem um controlador de memória integrado, que desempenha operações de nivelamento de desgaste comuns, tais como coleta básica de lixo.

Outro tipo da memória supracitada se referem às unidades Flash USB, que foram criadas em 2002 e propiciam uma combinação de taxas de transferência mais céleres e uma maior capacidade em um formato menor. Estas foram idealizadas como uma alternativa para CDs e unidades de disquete, a fim de se transferir informações rapidamente de um computador para outro. Uma unidade flash USB traduz-se em um conector USB, um controlador de memória e o chip de memória flash NAND.

Por fim, a terceira modalidade de memória flash concerne a uma unidade de estado sólido (SSD), que é um dispositivo de armazenamento produzido em 2007, possuidor de capacidade muito maior do que os cartões SD ou a memória flash USB. Estes surgiram para substituir as unidades HDDs tradicionais, se utilizando de formato e interface similar e, assim, são tranquilamente substituíveis na maior parte dos sistemas de computador. Atualmente, elementos menores foram feitos para encaixar os SSDs em hardware ainda menor e mais fino. O controlador SSD irá gerenciar as funções como nivelamento de desgaste intensivo dependente do fabricante e coleta de lixo. Cabe afirmar que os SSDs são operados em computadores desktop, notebooks, servidores e sistemas de armazenamento.

Nesse sentido, sobreveio a interligação entre a memória flash e a computação forense. De início, cabe salientar que a ciência forense se trata do método científico de coletar e verificar informações sobre fatos passados, sendo estas utilizadas em um tribunal de justiçaÉ coletada uma evidência a fim de se originar uma ligação entre um crime e um suspeito, para que possa restar comprovada sua culpa ou inocência. Com o intento de produzir evidências confiáveis, é necessária a observação de três conceitos, quais sejam, cadeia de custódia; admissibilidade de testes, evidências e testemunhos; e testemunho de peritos.

Primeiramente, há a cadeia de custódia, que irá descrever, com cautela, a documentação e avaliação de qualquer tipo de evidência. Algumas formas de evidências não podem ser conservadas indefinidamente em face de sua natureza, como, por exemplo, um corpo humano e restos de pingos de sangue, ou, ainda, existem outras que podem ser destruídas durante a análise, como exames de sangue para medicamentos, de modo que estes necessitam de uma devida documentação e avaliação. A partir dessas evidências, com documentos e imagens, haverá a viabilidade de se reavaliar as evidências a qualquer instante. É preciso que haja provas sobre o local seguro em que as evidências foram armazenadas até o momento da descoberta, de maneira que cada alteração de localização da possível prova deve ser documentada. Caso esta documentação apresente lacunas no tempo, a evidência poderá ser renegada e será inadmissível para o tribunal.

Por sua vez, a admissibilidade de testes, evidências e testemunhos diz respeito a existência de padrões legais para a admissibilidade de provas forenses e testemunho de especialistas. Um tipo de padrão legal para este fim referente a admissibilidade da evidência forense se trata do padrão Frye, o qual assegura que a técnica forense em tela deve possuir a anuência geral da comunidade científica.

Finalmente, o terceiro conceito se refere a testemunha de especialista, ou testemunho de peritos. Em qualquer investigação, pode existir uma testemunha de fato, que, via de regra, irá narrar os fatos observados por esta, e uma testemunha especializada. O perito possui experiência própria dentro de uma determinada disciplina e tem plena capacidade de dar opiniões referentes à disciplina tratada. É necessário o reconhecimento e qualificação oficial da testemunha especializada, o que envolve um processo legal, via de regra.

Existem algumas evidências denominadas evidências digitais. Para Eoghan Casey, evidências digitais são quaisquer dados guardados ou transmitidos que podem constituir um nexo entre um crime e uma vítima ou um suspeito ou tenham a viabilidade de provar a ocorrência de um delito. Esses dados podem se basear em textos, imagens, áudio e vídeo, sendo alguns exemplos de evidências digitais os históricos de bate-papo, arquivos de e-mail, imagens, vídeos de vigilância ou arquivos de log que expõem o acesso a certos recursos.

Por vezes, nas situações em que um crime for executado no mundo real, as evidências podem ser encontradas virtualmente nos dispositivos digitais de um suspeito ou na internet. Os elementos que vigiam o mundo físico no dia a dia, como câmeras de tráfego, câmeras ATM e webcams, expande a possibilidade da internet, bem como as mensagens compartilhadas cada dia mais através das redes sociais, nas quais os endereços IP mostram a localização de uma pessoa e, inclusive, registram tais conversas e mensagens. Isto posto, a chance de êxito a partir de análises de evidência digital no andamento de uma investigação tem sido gradativamente maior.

Na análise, por especialistas em computação forense, de um meio digital, as evidências tem de, em sua maior parte, ser recuperadas através de dados destruídos, intencionalmente ou não, ou perdidos. No entanto, primeiramente, independentemente do estado da mídia e das informações, deve-se criar uma imagem que seja uma cópia digital do estado quando o dispositivo foi coletado.

Tal imagem comprovará a cadeia de custódia, a integridade da evidência possivelmente encontrada no curso da investigação, e, assim, será a prova de que os dados no meio não sofreram qualquer alteração por parte do investigador ou por um terceiro a partir do momento em que o dispositivo foi coletado até a sua apresentação em tribunal.

Esta verificação da integridade, via de regra, necessitará de uma comparação da impressão digital entre a imagem inicial e a evidência apresentada. Essa evidência digital se constitui, sobretudo, em um valor de hash da imagem, significando uma soma de análise armazenada dos dados. Logo, uma cópia ou imagem igual de um dispositivo terá impressão digital semelhante ao do original, de modo que uma pequena modificação causaria uma impressão digital distinta do original.

Após a aquisição de um dispositivo contendo memória digital, o investigador tentará coletar uma imagem digital do dispositivo restaurado antes de procurar por evidências. Em certos casos, tal etapa não é possível em face de falha de hardware de natureza intencional ou não intencional. Com isso, deverá ser inicializada uma recuperação baseada em hardware ou software.

No entanto, salienta-se que, durante a investigação de um crime passado ou em curso, os investigadores forenses possuem limitações legais para atuar. Assim, este contém regulamentos com a finalidade de tutelar a privacidade do público. Por esta razão, distinções entre as informações coletadas e as informações transmitidas são feitas, de forma que estas são consideradas mais privadas e, assim, mais protegidas por dificultar a obtenção de um mandado do que aquelas.

É mais trabalhoso resgatar informações da memória flash do que das unidades de disco rígido, posto que todos os chips de controle e memória são soldados em uma placa. Logo, não é possível apenas substituir uma parte do dispositivo sem encontrar o mesmo modelo exato e substituir peças através de uma nova solda. A depender do tipo de memória flash, de dois a vinte chips podem vir a permanecer em uma placa. A nova soldagem manual é um trabalho dificultoso e delicado e praticamente impossível para múltiplos chips.

Há, ainda, a possibilidade de não vender cada chip de memória e, assim, realizar a leitura de cada um separadamente utilizando ferramentas e hardware específicos. Tal viabilidade pode ocorrer tanto nos casos dos cartões de memória com um chip, como em SSDs, com vários chips, posto que esse método se torna muito complicado, tendo em vista que cada fornecedor se utiliza de estratégias distintas sobre como lidar com chips, como realizar o nivelamento de desgaste e coleta de lixo e como distribuir dados.

Ao tratar acerca de software para recuperação de HD, pode-se afirmar que a recuperação de informações nem sempre é relacionada ao hardware. Em muitas situações, a verificação do disco a partir de um software é satisfatória para resgatar dados de um disco. Assim, o arquivo real não é apagado das unidades de disco rígido e, ocasionalmente, será trocado por um novo arquivo. Isto é comumente feito para recuperar dados. Insta salientar que, ao restaurar informações de discos e coletar evidências, os dados originais tem de permanecer inalterados ou modificados o mínimo possível.

Os especialistas utilizam de um hardware especial para copiar bit a bit os dados no disco para um arquivo de imagem ou outro disco. Tal aparelho é denominado de bloqueador de gravação, sendo utilizado como conexão entre o disco rígido e o computador, além de supervisionar os comandos que estão sendo enviados e impossibilitar que o computador armazene os dados no disco. Enquanto os comandos de gravação estão sendo bloqueados, os comandos de leitura são transferidos para o dispositivo.

Conforme afirma Manun (2007), no que se refere às ferramentas de software forense, muitas ferramentas foram criadas para que a área forense pudesse ter formas de recuperar dados de unidades de disco rígido e outras memórias digitais, conjuntos de software caros e ferramentas de código aberto. Todavia, cabe mencionar que uma das ferramentas de coleta de evidências forenses mais famosas e tradicionais é o EnCase.

O EnCase tem a capacidade de copiar discos a partir da tecnologia de fluxo de bits a fim de produzir uma reconstrução virtual do sistema de arquivos. Outras duas ferramentas lastreadas em janelas diferentes são a FTK (Forensic Toolkit por Access Data) e X-Ways. Estas três ferramentas possuem como característica própria o armazenamento de dados adicionais com a imagem de disco como valores de hash MD5 a fim de comprovar a integridade da imagem.

Por sua vez, há o Sleuth Kit, que concerne a um conjunto de software de código aberto que é executado em istemas operacionais distintos e suporta todos os sistemas de arquivos

comuns. A autópsia é tida como uma plataforma forense digital e uma interface gráfica para o The Sleuth Kit e ferramentas forenses digitais diversas.

Após a visualização de um disco rígido usando a tecnologia de fluxo de bits, cada bit da unidade original será conservado no arquivo de imagem e pode ser analisado. Tais ferramentas supracitadas tem a chance de auxiliar o examinador a reunir possíveis evidências em arquivos existentes e, inclusive, podem restaurar dados de arquivos apagados ou partições formatadas. No entanto, cabe afirmar que essas ferramentas apenas são aptas a processar discos não criptografados, se o sistema de arquivos criptografados (EFS) for usado, de modo que poderá ser feita uma imagem, porém a análise dos dados intenta muito mais esforço.

Um importante fator acerca da recuperação de software da memória flash refere-se ao fato de que, para verificar um SSD e coletar evidências de arquivos existentes, a mesma tecnologia é utilizada como nos discos rígidos convencionais. Nesse sentido, o EnCase ou outra ferramenta apresentada é usada para capturar uma imagem do meio, na intenção de não modificar os dados originais e coletar possíveis arquivos de evidências.

Assim, os examinadores terão chances pequenas de resgate de dados, visto que as partições foram formatadas ou os arquivos foram apagados. Ao contrário do que acontece com as unidades de disco rígido, a memória flash e, sobretudo, as memórias SSDs possuem rotinas internas que não tem como ser influenciadas externamente, como, por exemplo, com um bloqueador de gravação.

Para Casey (2011), existem, assim, algumas ferramentas que podem ser utilizadas para capturar imagens e coletar potenciais evidências em SSDs são as mesmas que para HDDs. A leitura dos chips de memória simples de um SSD ou outra memória flash, nas situações em que há um problema de hardware ou para evitar rotinas internas ou modifiar os dados armazenados nos chips de memória, pode ser feita através de quatro ferramentas, quais sejam, o PC-3000 Flash SSD Edition (Recuperação de Dados ACE), Dumppicker, Extrator Flash, e Flash Doctor.

Estas ferramentas atuam de forma similar, posto que o hardware lê o conteúdo de um chip de memória e, então, o software compara o fabricante e modelo do chip com um banco de dados e ajuda no resgaste de informações já existentes. O ACE Data Recovery anunciou, há poucos anos atrás, uma colaboração estendida entre a empresa de recuperação de dados e a SandForce e a elaboração de um novo software específico para aperfeiçoar a recuperação de dados SSD baseada em SandForce.

Nesta senda, cabe afirmar que os fabricantes de controladores SSD encaram uma forte concorrência e, muitas vezes, não querem compartilhar o insight das rotinas internas, criptografia, nivelamento de desgaste e coleta de lixo. Dessa forma, a cooperação entre uma empresa de recuperação de big data e a maior fabricante de controladores SSD ainda é um passo a ser conquistado, da mesma forma como o fato de que aprimoramento para examinadores forenses e especialistas em recuperação de dados levou a um crescimento drástico da taxa de recuperação para SSDs com base em SandForce, de modo que são fatores a serem ainda bastante observados nesse contexto e merecem a devida atenção.

6. Conclusão

As inovações tecnológicas de memória introduzidas foram de extrema relevância no campo da recuperação de dados e investigadores forenses. No entanto, é possível afirmar que ainda há diferenças significativas entre modelos distintos e o fato de que a recuperação de dados

imprevisível tornou-se bastante repentina. Os testes de soma de verificação de unidades inteiras realizados por especialistas e aqui descritos e analisados podem constatar que as rotinas internas executadas em segundo plano em SSDs podem falsificar os resultados sem a viabilidade de desabilitá-los. É possível ver como a persistência de dados é variável entre os discos rígidos tradicionais e a memória flash. Logo, ao passo que as unidades de disco rígido, cartões de memória flash e dispositivos de memória USB seguem conservando informações mesmo após a exclusão, os dispositivos de memória SSD excluem de imediato 95 a 100% de todos os dados ou os tornam ilegíveis. Assim, insta salientar como a aquisição de dados na memória SSD é imprevisível e altera-se entre modelos e fabricantes distintos. Com isso, ainda não foi localizado nenhum método aceitável para aquisição de dados na memória flash, de modo que examinadores forenses não tem como seguir as diretrizes comumente utilizadas para processar e conseguir evidências digitais que podem ser atestadas como 100% não manipuladas. Houve uma época em que o problema ainda era irrelevante, porém a conscientização geral acerca do presente tema vem aumentando gradativamente e, assim, nota-se um primeiro passo indispensável, bem como estudos que servirão de embasamento para pesquisas futuras, a fim de que novos padrões e novas diretrizes para futuro sejam criados e consolidados na área forense.

Referências

A. A. Mamun, **Hard Drive Mechatronics and Control**, Boka Raton, FL: CRC Press, 2007.

E. Casey, **Digital Evidence and Computer Crime Third Edition**, Watham, San Diego, London: Academic Press, 2011.

ELEUTERIO, Pedro M. S.; LANGE, Rodrigo. **Tratado de Computação Forense**. Editora Millenniun: 1 ed, 2016.

G. B. Bell and R. Boddington, **"Solid State Drives: The Beginning Of The End For Current Practice In Digital Forensic Recovery?,"** *The Journal of digital forensics, Security and Law*, pp. Volume 5, Number 3, 2010.

S. MOULTON, **"Solid State Drives Destroy Forensics & Data Recovery Jobs**," Las Vegas, 2011.

S. MOULTON, **"Solid State Drives Destroy Forensics & Data Recovery Jobs**," Las Vegas, 2011.